Mert „az Élet él és élni akar” (89. rész)

A legtöbb gondunk és betegségünk kórokozója a tudomány által szaporított, a médiában terjesztett, hibás tudás. A hibás tudások legkártékonyabbja, hogy küzdjünk betegségeink ellen, mindenáron győzzük le a kórt...
A betegség a legjobb barátunk. Az Élet maga a változás, a betegség a Változásban segít bennünket. Ha megértjük üzenetét, százszor szebben, ezerszer erősebben élhetjük tovább életünket! Miben segít, miben gátol, milyen cél felé vezet? Miben kell változnunk a test, a lélek és a szellem szintjén?
Sorozatunkban ezekre a kérdésekre keressük együtt a választ, és aki keres - talál! (GG)

Egészségünk és a digitális kor veszélyei - 1. rész

Kedves Olvasó!

Új kalandra hívlak! A kaland játszóterülete pedig a digitális kor. Ez az a kor, amiben ma létezünk, és élni kényszerülünk, akár akartuk ezt, akár nem. Jogosan tehetjük fel a kérdést, hogy a rakétasebességgel felgyorsult fejlődéssel, a gyors generációváltással és értékkrízissel jellemezhető digitális forradalomban mit tehetünk saját, gyermekeink és unokáink egészségéért és jövőjéért? De folytathatjuk a sort: mit tehetnek a nevelők, pedagógusok, az orvosok, a testi-lelki-kapcsolati egyensúlyunkra vigyázók, a kulturális élet és az etikus-humánus kultúra védői? Mekkora tudásra van szükségünk ahhoz, hogy egyáltalán felfogjuk és megértsük, mivel is állunk szemben: egy mindenben kényelmünket szolgáló technológiával, vagy ennek égisze alatt egy lassan lopakodó és a végén az emberiséget robotizáló, teljes rabszolgasorsba taszító hatalommal?

Ha egy kicsit jobban belenézünk a digitális kor eszközállományába, lehetőségeibe, és azok alkalmazási területét szemügyre vesszük, önkéntelenül is egy közmondás jut eszünkbe: „alkalom szüli a tolvajt!” Igen, úgy tűnik, hogy a digitális kor eszközállományát nemcsak nemes célokra használják! Az elkövetkezőkben ezt a kérdést járjuk alaposabban körbe, megvizsgálva a hétköznapi embereket érintő veszélylehetőségeket vagy veszélyeket. Gyermekeimet mindig arra biztattam, hogy kerüljék a veszélyt! Miért? Mert egy veszélyes helyzetből még a tragédia is könnyebben szökken talpra!

A digitális technológia mindenre ráteszi a kezét, és a profit szolgálatába áll

A digitális technológia mindenre ráteszi a kezét, és a profit szolgálatába áll. Mindenről, mindenkiről, mindenhol és mindent begyűjt. A felhasználók viselkedéséről összeszedett adatokat feldolgozza, tárolja, első lépésben eladja a hirdetőknek, majd pedig tömegméretekben befolyásolja a felhasználókat.

Miért van szükség a befolyásolásra? Azért, mert ha a vásárlók várható viselkedését előre tudom jelezni, akkor az profitnövelő tényező. Ezért az elemzések alapján ebbe a célsávba tereli a leendő vásárlókat és befolyásolásával potenciális vásárlóvá alakítja azokat. S mindezt globálisan!

Nos, Kedves Olvasó, ez a nyers valóság, ez az alap, innen kell továbbjutnunk valahova, békésebb vizekre. Miért? Azért, mert életünket jellemző szokások, apró kis titkaink a magánéletünk részei, és legfeljebb azokra tartoznak, akikkel megosztjuk azt. Az állandó jellegű adatgyűjtés eredményeképpen, ellenőrizhetetlenül olyan dolgok is idegen kezekbe landolhatnak, ami számunkra nem kívánatos, és ha tudnánk róla, akkor tiltakoznánk és letiltanánk. Arra pedig végképp nincsen garancia, hogy ezekből az adatokból egyszer nem egy olyan összeállítást készítenek, amely elemeiben igaz, de összességében nem. Ez kimerítheti az emberi méltósághoz való jog megsértését, beláthatatlan bonyodalmakat, anyagi és erkölcsi kárt okozhat. Ezek mindegyike pedig alapvető összefüggésben áll egészségünkkel. Ezen módszerek felismeréséhez, és esetleges kivédéséhez pedig tudásra van szükségünk. Nincs módunk arra, hogy ilyen szűk keretek között mindent és kellő mélységben megvizsgáljunk, de néhány dolgot azonban kivesézhetünk. A mobiltelefonokkal kezdjük, majd a laptopokat is megvizsgáljuk.

Amikor ezt a cikket írjuk, a Föld lakossága több mint 7 milliárd és 600 millió ember,

Ha a vásárlók várható viselkedését előre tudom jelezni, akkor az profitnövelő tényező

Az emberek nagy része el sem tudja képzelni napját mobilkészülék nélkül

miközben a mobiltelefonok számát 9-10 milliárd készülékre becsülik. Figyelembe véve a mobiltelefonok használatának területeloszlását, nyugodtan mondhatjuk, hogy sok embernek két vagy több mobil készüléke is van. Mindez a technikai és a fogyasztói társadalom fejlettségének egyik mutatója. De vajon hány felhasználó tudja, hogy mit hordoz a zsebében? A technikai fejlődés alakítja a társadalmat, mindig is alakította, de ilyen léptékű és ilyen gyors átalakítás még nem volt az emberiség történetében! Az emberek nagy része el sem tudja képzelni napját mobilkészülék nélkül! Az okos telefonok megjelenésével pedig az alkalmazások köre felfoghatatlan módon kiszélesedett, felgyorsult, és egyre fontosabbá vált. A beszélgetés szinte már csak mellékes tevékenység. Ezen készülékeken zajlik az emberek mindennapi életének zöme, az állandó „jelenlét” biztosításától a helymeghatározáson át, a vásárlásoktól, a banki szolgáltatások igénybevételéig minden.

Vajon megbízhatunk-e a mobiltelefonunkban, amelyek olyan sokat tudnak az életünkről, hogy el sem tudjuk képzelni, mi több, bele se gondolunk, vagy bele se merünk gondolni, hogy igazából egy high-tech spionnal élünk együtt. A bennünket azonosító és rólunk mindent tudó chip nem a bőrünk alatt van, hanem egy kicsit nagyobb méretben, a zsebünkben hordjuk. Igen Kedves Olvasó, szembe kell néznünk a valósággal, önként spiont hordozunk a zsebünkben! Ahhoz azonban, hogy a használattal járó kiszolgáltatottságunkat megértsük, meg kell ismernünk a mobil készülék alapvető felépítését, és valamelyest a mobil hálózatot is. Ez nem egy óriási feladat, kis figyelmet igényel és már el is sajátítottuk a lényeget. Nos, most alapfokon megvizsgáljuk, a készüléket és a hálózatot is, mind a két esetben a hardver felépítését és a szoftvertműködését is.

1. A mobiltelefon egy rendkívül high-tech készülék. Az egy kis számítógép, de nem is egy mikro-számítógép van a mobiltelefonban, hanem három. A mai jobb mobiltelefonok teljesítőképessége jóval nagyobb, mint azé a számítógépé, amelyikkel a Hold expedíciókat véghezvitték. Nézzük meg ezt a három kis számítógépet részletesebben. A SIM kártya [2]. Ez az egész mobil telefon agytrösztje, amint később látni fogjuk. Ezen tudunk tárolni egy csomó telefonszámot, nevet, stb. és sok SMS-t. A SIM kártyán futó szoftvert (melynek pontosabb neve firmware) a szolgáltató távolról tudja újabbra cserélni. Ez a program egy kis memóriában (RAM) fut és egy központi processzor (CPU) hajtja végre. A SIM-kártya végzi a mobil hálózaton használt titkosítást is. Az egész rendszer egy „fekete doboz”, nem nyilvános, és nem tudjuk, hogy milyen szoftver fut ott, és pontosan mit is tesz. A privát szféra szempontjából jó tudni, hogy világszerte a SIM kártyát és a mobil készüléket egyedileg (IMSI, IMEI) azonosítják. (Így a mobil tulajdonos személyre szólóan azonosítva van.)

2. A Rádió egység, nevezik modemnek is, vagy baseband egységnek is [3]. Ez az egység felelős a mobiltelefon és a mobilhálózati adótorony közötti adatátvitelért, mindkét irányban. Átalakítja a rádió jeleket digitális jelekké a mobiltelefon további részeinek, és fordítva. A benne futó operációs rendszer teljesen ismeretlen, „fekete doboz”, a mobiltelefon legveszélyesebb része a privátszféránk szempontjából. Mivel a kommunikációs hatóságnál engedélyeztetni kell ezt az egységet, ezért a mobiltelefont gyártók néhány cégtől vásárolják meg az adott chip-et, amelyek a modemet gyártják.

3. A felhasználói számítógép. Ezen fut a mobiltelefon operációs rendszere és az

Igazából egy high-tech spionnal élünk együtt

Ha a mobiltelefonunk WiFi vagy GPS modult is tartalmaz, akkor a pozíciónk akár 5 m-re behatárolható

összes egyéb program, az alkalmazások (appok). Ennek a teljesítőképessége a mérvadó a telefon gyorsasága szempontjából. A mobiltelefonokon futó operációs rendszer piaca mára letisztult, az egyértelmű császár a Google Android, 2016 3. negyedévében 87,5%-os piaci monopóliummal.

Hogyan is működik a mobiltelefon hálózat?

A mobil készülékek a bázis állomások mobilhálózati adótornyaival, az URH sávba tartozó rádióhullámokkal kommunikálnak. A cellák mérete és így az adótornyok sűrűsége a geológiai és urbanisztikai adottságoktól függ, azt is figyelembe véve, hogy egy adótorony véges számú mobil készüléket tud kiszolgálni. Így a nagyvárosokban nagyon sok bázisállomás van. Az adótornyok, un. helyi kapcsolóközpontokkal vannak összeköttetésben, amelyek egymással összekapcsolva képezik az országos hálózatot. Ebben a hálózatban az egységek az SS7 (Signaling System Number 7) nevű protokollal kommunikálnak egymással, erről a későbbiekben lesz még szó. A szolgáltatókhoz tartozó hálózatok praktikusan az egész ország területét lefedik.

A mobiltelefon egyszerre több alapállomás jeleit veszi és annál az adótoronynál jelentkezik be, amelyiknek a térereje a legnagyobb. A bejelentkezéskor a mobil készülék az IMSI-t, és az IMEI-t köteles megadni. Fordítva azonban a toronynak nem kell azonosítania magát a mobil készüléknél, következmény: az IMSI elfogó (catcher), ld. később. Ahogy térben és időben mozgunk, mindig más toronynál jelentkezik be a mobiltelefon, ezáltal a mozgásprofilunk azonnal előáll.

A helyzet ennél azonban rosszabb, mert mobiltelefonunk rádiójelét nem csak egy alapállomás, hanem több is veszi, különböző térerővel. Három adótorony által vett jelek erőssége alapján a földrajzi pozíciónk - csak a rádióhullámok alapján - meghatározható, alaphelyzetben kb. 270 m pontossággal, de több alapállomás együttműködése eseten akár 25 m pontossággal is! Ha a mobiltelefonunk WiFi vagy GPS modult is tartalmaz, akkor a pozíciónk még nagyobb pontossággal is lekérdezhető, akár 5 m-re behatárolható. A fentieket összefoglalva, a „fekete dobozok” a mobiltelefonban, az SS7 protokoll, a IMSI, IMEI, a pozíciónk meghatározhatósága a privátszféránkat teljes mértékben likvidálja. Ha mobilt használsz, a privátszférádat elfelejtheted, pedig még meg sem vizsgáltuk részleteiben, a fentiek által okozott problémákat!

Problémák a mobiltelefonnál

A mobiltelefonokat úgy kellett készíteni, hogy segélyhívás SIM kártya nélkül is leadható legyen. Ez bármilyen hasznosnak tűnik is, egy rendkívüli problémát jelent. Ahhoz, hogy egy segélyhívást SIM kártya nélkül le tudjunk adni, több dolog szükséges. Először is, a mobiltelefonnak SIM kártya nélkül be kell tudnia jelentkeznie akármelyik adótoronyhoz. Be is jelentkezik: „Itt az IMEI-m, SIM kártyám az nincs!”. „OK”, válaszolja a torony. De ettől kezdve a nyomkövetés már meg is történik, ha esetleg csak 270 m pontossággal is. A második probléma ott jön, hogy a mobiltelefon rádió-egységének, az alapsávi egységnek, anélkül, hogy a fő vezérlő, a SIM kártya a telefonban lenne, hozzá kell férnie a mikrofonhoz és a hangszóróhoz. A telefon azonnal egy poloska lett! Mivel a Rádió-egység egy „fekete doboz”, tehát, bármi megtörténhet!

(Csak röviden írjuk le, hogy ennek a csak IMEI-vel való bejelentkezésnek egyenes következménye, ha van egy laptopunk, vagy táblagépünk, amiben van GMS/UMTS modul, anélkül, hogy SIM kártyát tennénk a készülékbe, a modul máris bejelentkezik egy adótoronynál, ha a készüléket bekapcsoljuk. Öngól a privátszférának. A sok visszaélés miatt egyes országok a SIM kártya nélküli segélyhívás lehetőségét megszüntették, pl. Németország.)

Problémák az azonosítással

A mobiltelefon kapcsolatfelvevő egysége az IMSI elkapó (catcher). Mivel a mobiltelefon a legerősebb jelet adó toronyhoz jelentkezik be anélkül, hogy az alapállomás azonosítaná magát, lehetőség van „hamis” (fake) alapállomásokat készíteni. Az IMSI elkapó egység magát a mobiltelefon felé egy alapállomásnak adja ki, az igazi adótorony felé pedig egy mobiltelefonnak. Ezzel tehát a mobiltelefon és az alapállomás közé ékelődik, mindenféle forgalom rajta keresztül fut, tehát lehallgatható. Ezek az egységek arra szolgálnak, hogy a mobil beszélgetéseket a titkosszolgálatok, rendőrség, hackerek, stb. le tudják hallgatni. De például egy tüntetés résztvevőit lehet egy IMSI elkapóval azonosítani, az összes

A mobiltelefon egyszerre több alapállomás jeleit veszi és annál az adótoronynál jelentkezik be, amelyiknek a térereje a legnagyobb

résztvevő mobilja várhatóan ebbe az egységbe jelentkezik be, ha ez adja a legerősebb jelet. Ráadásul ezek az IMSI catcherek manapság már aktatáska méretben készülnek.

Problémák a SIM-kártyával

Lássuk most a SIM-kártya révén adódó problémákat. A SIM kártyára lehet „csendes”(silent, „lopakodó” vagy szerviz) SMS-t küldeni. Erről az SMS-ről a felhasználó semmi jelzést nem kap, tehát az SMS se hangot nem ad, se a képernyőn nem jelenik meg. Ilyen „szerviz” SMS-el a mobiltelefont át lehet programozni. Pl. úgy, hogy amikor kikapcsoljuk, akkor azt gondoljuk, ki van kapcsolva, csak közben a mikrofon bekapcsolódik, és a környezeti hangokat egy - a „csendes” SMS által megadott telefonszámra továbbítja a tudtunk nélkül. Vagyis egy tökéletes lehallgató készülék lett a mobilunkból. Minderről pedig mi nem veszünk tudomást. Már 2003-ban ezzel a módszerrel csapott le a New Yorki-i rendőrség egy maffia klánra. További példa, hogy egy „csendes” SMS-el a telefon a pillanatnyi pozíciót megadott időnként egy megadott telefonszámra továbbítja a tudtunk nélkül. A legegyszerűbb formája a „csendes” SMS-nek, amikor csak a telefon pillanatnyi pozícióját, a tartózkodási helyét, akarják meghatározni, és a kommunikációs lépések a mobiltelefon és a torony között azonnal megadják a pozíciót. A német hatóságok ezt a módszert rendszeresen használják. Az egyéb lehetséges problémákra még sok példát tudunk felhozni.

Problémák a kommunikációs protokollal, SS7

Az SS7 protokollal kommunikálnak a helyi mobilhálózati kapcsoló központok egymással ugyanazon szolgáltató esetén, a különböző szolgáltatók egymással országon belül, és az összes szolgáltató a világban. A protokoll azonban nem tartalmaz azonosító lépéseket elegendő mértékben. Így bárki, aki az SS7 hálózathoz hozzáfér (és ez a kör széles lehet), szinte hihetetlen dolgokat hajthat végre bárkinek a mobiltelefonján! Mindehhez csak a mobiltelefonszámot kell ismerni. Néhány lehetőség, amit le lehet kérdezni: a mobil készülék pozíciója, az aktuális beszélgetés titkosítási kulcsa, a telefon tarifája, a felhasználó adatai, stb... Továbbá amit meg lehet változtatni: a felhasználó adatait a felhasználói adatbázisban, a telefonhívások, SMS-ek és adatok forgalom átirányítása (= lehallgatása) vagy letiltása, ezzel a telefonszámmal hívás létrehozása, SMS küldése, adatátvitel, stb. stb. Mindez a GMS/UMTS hálózatok esetében így működött! Az LTE hálózat esetén a protokollon ugyan javítottak, új nevet kapott, de a fenti alapvető problémákat nem küszöbölték ki. Mivel a világ egésze még nem állt át a legújabb technikára, a fenti problémákkal még egy ideig együtt kell élnünk. Öröm a hackereknek, titkosszolgálatoknak. Ne felejtsük, hogy a világ pénzügyileg és szakszemélyzettel legjobban felszerelt és legerősebb hackercsapata az NSA.

Hogyan védekezhetünk e problémák ellen

A SIM-kártyával és a modemmel kapcsolatos problémák lokálisak, a mobiltelefonban vannak. A „csendes” SMS-ek, a SIM kártya átprogramozása és a Rádió-egység nem ismert aktivitása ellen kizárólag akkor tudnánk védekezni, ha a SIM kártyán és a Rádió-egységen futó operációs rendszer nyílt forráskódú lenne. Ez lehetőséget adna egyrészt annak ellenőrzésére, hogy ezek az egységek pontosan mit is tesznek, másrészt

A „csendes” SMS-ek a mobiltelefon és a torony között azonnal megadják a pozíciót

A fólia egy Faraday kalitkát képez, amin a mikrohullámok sem tudnak áthatolni, ezért a mobiltelefon nem lesz elérhető

ennek ismeretében lehetne olyan operációs rendszert készíteni a mobiltelefonra, amely jelzi a nem kívánatos aktivitásokat (csendes SMS-t kaptunk), ill. ezeket nem is engedélyezi (a SIM kártya átprogramozása). De például biztonsággal le tudnánk kapcsolni a rádió-egységet, ha akarjuk. (A „Repülőgép” üzemmódról nem tudjuk pontosan, hogy is működik.) Mivel a két szoftver zárt forráskódú, szigorúan őrzött titok, így egyrészt védekezésünk korlátozott, másrészt joggal feltételezhetjük, hogy tudatosan zárt forráskódúak, a mobiltelefon a lehallgatásunkra is készült. Jogos feltételezésünket alátámasztja, hogy az alapsávi (Baseband) egységre már készült szabad szoftver a privátszférát támogató önkéntes szoftverfejlesztők által, amely ezen egység valamennyi funkcióját realizálja.

Az SS7 protokoll a mobilhálózati kapcsoló központokat, ill. a mobilszolgáltatókat köti össze. Ezekhez a berendezésekhez nincs hozzáférésünk. Így elvileg is lehetetlen az SS7 protokollban lévő „hibák” ellen védekeznünk. Tudomásul kell tehát vennünk, ha mobiltelefont használunk, az SS7 által okozott veszélyeknek, lehallgatási lehetőségeknek ki vagyunk szolgáltatva, azaz semmit nem tudunk ellene tenni. Kivéve egyet: nem használunk mobiltelefont! Ez természetesen nagyon kemény követelmény lenne. Pillanatnyi megoldás rövid időszakokra az, hogy a mobiltelefon akkuját kivesszük! Ezzel a mobil működésképtelen persze, így az esetleges lehallgatásokra is az. (Ha csak nincs benne egy kisméretű telep.)

Másik lehetőség az, hogy a mobilt jó vastag alufóliába tekerjük be. A fólia egy Faraday kalitkát képez, amin a mikrohullámok sem tudnak áthatolni, ezért a mobiltelefon nem lesz elérhető. Persze, így használni se lehet. De véd az adott időben a fenti problémák ellen. Ha a mobilunk olyan, hogy az akkut nem lehet kivenni belőle, akkor sajnos csak az alufólia segít. A kicsit felhasználóbarátabb mobiltelefon, ahol a Rádió-egységet, a mikrofont, WiFi-t fizikai kapcsolóval üzemen kívül tudjuk helyezni még várat magára [20], és nagyon drága lesz. Bár ezen már egy Linux operációs rendszer fog futni!

A mobiltelefonok operációs rendszere

A mobiltelefonok különböző operációs rendszerrel (OS) futnak. Az legelső mobiltelefonokkal, (pl. Nokia 1210) csak telefonálni és sms-t lehetett küldeni. Volt rajtuk ébresztő funkció, ami akkor is működött, miután kikapcsoltuk a telefont. Azaz igazán nem kapcsoltuk ki, de nem tudtuk, mit is kapcsoltunk ki. (Ennek a funkciónak rögtön aggodalmat kellett volna keltenie bennünk, hiszen ez jelzi, van rá lehetőség, hogy kikapcsoljuk a mobilt, és mégse kapcsoltuk teljesen ki.) Mindaddig, amíg a mobil ilyen egyszerű funkciókkal rendelkezett, csak a mobilhálózati szolgáltató és a nyomozó ill. hírszerző hatóságok tudtak bennünket lehallgatni, nyomon követni.

Az igazán nagy problémákat az okostelefonok megjelenése hozta. Ezzel szinte egy időben az akkori legújabb telefonokban már volt egy kamera a hátlapon, egy második később megjelent az előlapon is, hogy videó telefonálást tudjunk végrehajtani, ha a pénztárcánk engedte; megjelent a GPS vevő a mobilban, ezzel a földrajzi pozíciónkat akár 5 m pontossággal meg lehetett határozni. A privát szféra szempontjából az okostelefonok legrosszabb tulajdonsága, hogy képesek lettek az Internetre kapcsolódni WiFi vagy mobil adatforgalom révén. Az Internet megjelenése a mobiltelefonokon nem csak kényelmet jelentett, böngészhettünk, e-mailt olvashattunk, hanem egy jelentős veszélyt is. Az operációs rendszer, amely már igen komoly szoftver volt, elvihette a telefonról az adatainkat, sőt, az egyes alkalmazások is megtehették ugyanezt. Az okostelefon tehát a privátszféra elsőrendű ellenségévé lépett elő. Szinte valamennyi alkalmazás egyet akart, minél több adatot gyűjteni, akár csendben, akár hivatalosan. (folytatjuk)

A cikkben használt rövidítések magyarázata:

SIM kártya: A SIM-kártya egy olyan integrált áramkört tartalmaz, mely biztonságosan tárolja az azonosítót és egyéb kódokat.

IMSI: International Mobile Subscriber Identity, (Nemzetközi mobil előfizető azonosító)

IMEI: International Mobile Equipment Identity (Nemzetközi mobil készülékazonosító)

GSM: Global System for Mobile Communication (Globális mobil kommunikációs rendszer)

UMTS: Mobile Universal Telecommunications System, (Univerzális telekommunikációs rendszer)

LTE: Long Term Evolution kifejezésből, tükörfordításban „hosszú távú fejlődés”

GPS: Global Positioning System (Globális Helymeghatározó Rendszer)

LINUX: nyílt forráskódú operációs rendszer, Linus Torvalds fejlesztőről elnevezve,

NSA: National Security Agency (US), (Nemzetbiztonsági Ügynökség)

Barátsággal,
Erdei István és Erdei Károly

www.magtar.hu